

read me



| Finn dine like-sinnede i Abakus

| Full Steam ahead

| Null motivasjon?
Null problem

Veien videre

Redaktør
Magnus Hanesand

Økonomi
Øyvind Monsen

Layoutansvarlig
Simen Holmestad

Medvirkende
Andreas Hammer Håversen
Marie Andreassen Svanes
Axel Martinius Kjønsberg
Jørgen Martin Syvertsen
Magnus Eide Schjølberg
Marius Sørensen Dreyer
Ole Kildehaug Furseth
Karoline Velsvik Berge
Ingrid Marie Sørensen
Kristina Hovland Berg
Henrik Fauskanger
Thale Finhammer
Tobias Skjelvik
Karoline Sæbø
Marie Hovland
Viktor Solberg
Eivind Kløvjan
Signe Carlsen
Helle Gråberg
Magnus Rand
Vegard Ervik
Ane Larsen

Kontakt
readme@abakus.no

readme, Abakus
Sem Sælands vei 7-9
7491 Trondheim

Nettutgave
readme.abakus.no

netcompany

Leder

Velkommen! Velkommen til Abakus, alle nye førsteklassinger. Velkommen tilbake til en relativt normal studiehverdag, alle andre. Og velkommen, alle og enhver, til min første utgave som redaktør. Og akkurat som redaktøren før meg så heter jeg Magnus, og skal lede **readme** det neste året.

Dette er et veldig rart semester å komme tilbake til. Koronakrisen avbrøt vårsemesteret vårt så altfor brått, og for mange er dette første gang på månedsvis at vi får møte studievennene våre igjen. Våren og sommeren har derfor vært en vanskelig tid for flere av oss, så nå er tiden for å være en ekstra god venn.

Når det er sagt, er det også tiden for å se fremover! Dere førsteklassinger aner ikke hvor heldige dere er som har Abakus som linjeforening. Søk komité, søk revyen, finn deg

en interessegruppe, dra på *bedpres*, dra på kurs eller bare heng på kontoret. Om du starter i første eller femte har ikke noe å si, engasjer deg i Abakus! Linjeforeningen er ikke mer enn medlemmene som utgjør den.

Verden er i stadig forandring. Nå som 01-kullet har ankommet, er det vel bare et spørsmål om tid før Abakus er på TikTok. Vi starter også på første fulle semester med ny organisasjonsstruktur. Heldigvis er det noen uforanderlige sannheter vi kan lene oss på: Trondheim er Norges beste studentby, ingen har så mye kontroll på livet som det ser ut fra utsiden, *exphil* er bare tull, Bjørn Johan Muri er en nasjonalskatt og det blir alltid seks utgaver med **readme** i året.

Redaktør

Magnus Hanesand

I denne utgaven

4 Guide til verv og interessegrupper



12 Anmeldelse av «Being A DIK»



18 Snilt deg gjennom drømmestudiet



Karakterer til besvær

Tekst: Andreas Hammer Håversen
Foto: Henrik Fauskanger

Som studenter på NTNU er vi godt vant med trege sensorer og brutte sensurfrister. Det er jo en juletradisjon at eksamenskarakterene fra høstsemesteret kommer en uke for sent. Noen ganger går det imidlertid for langt. Hva ville du sagt om det hadde gått nesten ett år siden innlevering og du ennå ikke hadde fått karakteren din?

Det er akkurat det som har skjedd med flere masteroppgaver fra våren 2019. **readme** erfarer at minst fem masterstudenter ikke fikk sensuren sin før i år, til tross for at sensurfristen for masteroppgaver er tre måneder etter innlevering. Vi erfarer også at instituttet nærmest har ignorert de rammede når det gjelder purring og ny informasjon. Minst én person opplevde total stillhet fra offisielt hold i tre måneder. Dette er helt uholdbart.

Masteroppgaven, som vi skal bruke nesten et halvår av livene våre på, er et enormt arbeid som det står stor respekt av. Da bør IDI og fakultetet være i stand til å gjengjelde den respekten, og gi et resultat i rimelig tid.

Gi meg det jeg vil ha: respekt
Riktig nok er det ikke veldig mange som har et enormt behov for den karakteren. Vi er velsignet med å ta et studie der De fleste™ får seg jobb uansett hvordan vitnemålet ser ut. Det kan likevel skape problemer dersom selskapet man er ansatt hos gir mindre lønn om man ikke har oppnådd mastergrad. En annen utfordring er når bedrifter må permittere. Da er nyansatte uten vitnemål og formell kompetanse blant de første ut døra. Konsekvensene av senzur kan med andre ord være enorme.

Nå må IDI og fakultetet gå i seg selv og finne ut hvorfor dette har skjedd. De har ikke et rykte på seg for å være raske med sensur, men dette er ekstremt. En utmatrikulert masterstudent skal ikke måtte vente et helt år på sensuren på mastergraden sin. Det betyr i realiteten at de aldri blir ferdige som studenter, siden de ikke får utlevert vitnemålet før sensuren er ferdig.

I speideren sier vi «En gang speider, alltid speider». IDI later til å ha tatt slagordet «En gang student, alltid student». Livslang læring er viktig, men vi kan ikke være studenter for alltid. IDI må sørge for at masterstudentene får den sensuren de har krav på.

I tide.

Engasjer deg i Abakus

Tekst: Ane Larsen og Magnus Schjølberg
Layout: Marie Hovland

Liker du banan? Da passer du nok godt inn i Abakus. Ikke? Du passer nok godt inn likevel. Ved første øyekast kan kanskje Abakus virke som en pretensiøs gjeng med røde bånd og *daljer*, som det kan være vanskelig å bli en del av. Men heldigvis er linjeforeningen vår bredere enn det, for Abakus er mye mer enn bare Hovedstyret og komiteene. I Abakus digger vi alt fra klatring og Smash, til Pepsi Max og revy – du vil ikke tro hva slags interesser som kan binde oss abakuler sammen.



Revyen

Hvert år setter Abakus opp sin egen revy, som, fra et rent objektivt standpunkt, naturligvis er Trondheims beste. For å sette opp en så god revy kreves en stor gjeng abakuler med forskjellige interesser og egenskaper. Revy er nemlig mye mer enn bare det som skjer på scenen, så her har alle noe de kan bidra med. Uavhengig av hvilken revygruppe du blir med i, er det alltid rom for mye kreativt arbeid: leke med laser, sy *fleshlights* i menneskestørrelse eller starte *beef* med Omegarevyn.

Vervet varer kun ett år av gangen, og er en unik mulighet for å bli kjent med abakuler på tvers av linjer og klassetrinn. Opptak skjer tidlig på høsten, og alle som vil få være med i en gruppe. På høstsemestret er det fokus på sosialisering og planlegging, mens på vårsemestret gjennomføres innspurten til revyforestillingene i mars.

Ababand

Abakus har faktisk et eget linjeforeningsband som opptrer på både våre egne arrangementer samt tar på seg eksterne spillejobber. Ababand er lavterskel og gøy, og fallhøyden er lav. Perfekt for deg som har spilt i band før, eller som alltid har hatt lyst til det. Når opptaket er og hvem man ser etter varierer fra år til år basert på hvilken besetning bandet har, men det er alltid mulig å sende en mail til ababand@abakus.no for å melde sin interesse!

UNDERGRUPPER

AbelLan

AbelLan er en undergruppe for spillinteresserte abakuler. De arrangerer LAN to ganger i semesteret, pluss FadderLan på høstsemestret. I tillegg kjøres det mange konkurranser i løpet av året, blant annet i «League of Legends», «Smash», «Paint» og «Rocket League». Her kan man melde seg på som enkeltspiller eller som lag, også med deltagere fra andre linjer. AbelLan sørger for billig snacks og pizza, så dette gjelder det å få med seg.



Oss som spiser banan



AbaMat

AbaMat er en samling abakuler som elsker mat. Om man foretrekker å lage mat eller spise den, skiller det ikke på her. Gruppa har per mars 2020 litt over 300 medlemmer, så det er tydelig at abakuler er glade i mat. En ting mange abakuler ikke er så glade i er derimot eksamsperioden. Heldigvis lyser AbaMat opp denne mørke tiden ved å invitere til middag hos hverandre. Her kan matinteresserte abakuler nyte god mat og bli bedre kjent.

Oss som spiser banan, også kjent som OSSB, er interesseggruppa for bananglade abakuler. Interesseggruppa ble startet opp for å vise hvor lavterskel interesseggrupper faktisk kan være, og at man kan samle en gjeng abakuler om nesten hva som helst. De arrangerer bananorama på kontoret, et spennende arrangement som involverer spising av bananer. «Men hva om jeg ikke liker banan?» tenker du kanskje. Heldigvis åpner OSSB for et bredt spekter av medlemmer, alt fra de som liker banan til de som ikke gjør det.



AbaSmash

Om du liker «Super Smash Bros.», så er Abakus rett sted for deg! Helt siden spillet ble innført på linjeforeningskontoret i 2015, har det vært en essensiell del av mange abakulers hverdag. Få aktiviteter har blitt like representative for Abakus som det «Smash» har. Det skal godt gjøres å finne et tidspunkt av døgnet hvor spillet ikke er synlig på kontorets TV-skjerm. Om den daglige «Smash»-iveren ikke er nok for deg, arrangerer AbaSmash også en prestisjefull turnering hvert semester som trekker en god andel tilskuere.

INTERESSEGRUPPER



PPP

«Alle liker pizza, de fleste liker pils, ikke alle liker Paradise Hotel. Kombinasjonen Pizza, Pils og Paradise er derimot uslæelig.» – Pizza, Pils og Paradise på Facebook. PPP møtes på kontoret én gang i uka for å spise pizza, drikke pils og se på Paradise Hotel. I senere tid har også *Ex on the Beach* fått sin skjermtid på kontoret, noe som også viser seg å engasjere. Den uslæelige kombinasjonen klarte forrige sesong å samle en gruppe på mellom fem og tjue abakuler i uka. Jo flere som møter opp, desto billigere blir pizzaen. Kontoret kan til og med by på en helt egen gullkule plassert i glasskapet, som symbol på at PPP alltid fortjener en plass i Abakus.



AbaPluss

AbaPluss er en interessegruppe for abakuler med interesse for finans og sparing. Gruppa har en Facebook-side hvor det diskuteres aksjer, fond, finansielle instrumenter, aktuell markedssituasjon og mye annet innenfor finans. I AbaPluss er det fokus på læring, og det skal være lav terskel for å stille spørsmål og presentere ideer og meninger.



Abakatter

Navnet på gruppa er et dårlig ordspill på apekatter, som de færreste forstår uten mer kontekst. Gruppa samles rundt en felles interesse for buldring, altså innendørs klatring uten tau. Her kreves det absolutt ingen forkunnskaper. Det eneste man trenger av utstyr er klatresko, noe man enkelt kan låne på klatresenteret. Gjengen sponsers av Abakus, og får støtte til to klatreinnganger i måneden, noe som reduserer prisen per hode fra 110 til 50 kroner. Utenom de faste klatreøktene postes det jevnlig innlegg på Facebook av abakuler som søker klatrepartnere. Interessert i å klatre din vei inn i Abakus-samholdet?

C2 - Faringsskriv fra student- livet

Dette skrivet er skrevet av tre jenter som gikk ut fra data våren 2020. Etter fem lange og korte år, ønsker vi å dele noen erfaringer med dere som enda har den beste tiden i livet foran dere.

Skriv: Signe Carlsen,
Marie Andreassen Svanes og Kristina Hovland Berg
Layout: Kristina Hovland Berg

Tid

● Alkohol er dyre dråper i Norge, og som fattig student med høyt alkoholkonsum kan du fort ende opp på Luksusfellen. Men du trenger ikke være avholds av den grunn, for på både Europis og Elgeseter Minimarked kan du skaffe vinlagingssett for under 500-lappen. Med litt tålmodighet har du 23 liter med hjemmelaget vin ferdig før det har gått to uker. Fyll på i tomme brusflasker, og du er klar for vors uten å måtte bekymre deg hverken for lommebok eller ølsalg.

● Utnytt at vi i Abakus har mulighet til å dra på flere bedriftspresentasjoner og kurs i ukens. Her får du ikke bare gratis mat og drikke, jobbmuligheter og faglig påfyll: Arrangementene er en gyllen mulighet til å bli kjent med nye folk. Du kan ende opp i samtale med både bedriftsrepresentanter og andre abakuler du kanskje ikke hadde blitt kjent med ellers.



Studier

● Det kan være svært stressende å begynne på nytt studie. Heldigvis er det vanskeligst å komme inn på NTNU, så det verste er faktisk overstått. Er du likevel stresset, må du egentlig først som sist bare slå deg til ro med at det alltid finnes noen på NTNU som er bedre enn deg i et eller annet, enten det er matte, løping eller gaming. Dette kan være vanskelig å akseptere dersom du var blant de beste på videregående. Da hjelper det å tenke at det alltid er noen som er *dårligere enn deg også*. Om du stryker i *matte 1* så er ikke det verdens undergang! Det finnes andre som har strøket fire ganger allerede og klarer seg fint for det.

● I starten av studiet kan det også være lurt å gå i forelesninger, både for å bli kjent med andre og å se hvem som går i klassen din. I tillegg finner du ut hvilke forelesninger som er nødvendige å gå i og hvordan du lærer best. Dette er en god mulighet til å finne ut hvem man kan jobbe godt sammen med, og de fleste er åpne for å bli med på lunsj eller i kollokvieguppe.

● Hvert semester får du et storstipend som skal brukes på materialer (bøker) som trengs til studiene. Som teknologistudent er det en ting man bør lære seg med en gang: Ikke kjøp bøker. De fleste finnes på nett, hvis ikke er det ikke verdt å ha dem. Neida. Finnes de ikke på nett kan du spørre eldre studenter, gjerne faddere, om de har PDF. Dersom du absolutt må ha fysiske bøker, kjøp for all del brukt via *ibok.no*, spør en fadder om de selger bøker eller lånn dem på biblioteket. Abakus har i tillegg en egen Facebook-gruppe for nettopp dette formålet: «Data/Komtekboek - Kjøp og salg».

● Ligger du litt dårlig an til eksamen? Gjør gamle eksamsensett. Ofte er forelesere så late at de ikke gir deres oppgaver i tillegg til å ikke gi informasjon om hvilke temaer som er viktige. Sjekk om konten er vanskeligere enn ordinær eksamen for å se om det er verdt å heller ta denne.



Sosialt

● På samme måte som når du søker jobb, så kan du få avslag når du søker deg til verv. Det kan virke som verdens undergang, men det er ikke alt. Du får heller tenke at det er deres tap, og at du kan søke deg til andre verv eller aktiviteter. Husk at for eksempel Abakusrevyen har opptak litt senere enn komitéoppbakene, og at Samfundet har opptak på både våren og høsten.

● Har du en merkelig interesse? Da er Trondheim perfekt for deg! Det eksisterer *alltid* en eller annen gruppe for den særlige hobbyen du har, og menneskene i denne gruppa setter nok pris på å møte flere likesinnede. Utfold deg selv og undersøk mulighetene!

● Om du synes videregående var et sosialt helvete, så vil studentlivet forhåpentligvis bli mye bedre. Som student er det lettere å møte likesinnede, enten via linjeforeningen eller andre studentgrupper, som aksepterer deg for den du er. Det viktigste for å danne nye vennskap er å snakke med nye mennesker. Det kan være skummelt i starten, men det kan gi deg stor fortjeneste.

● Dersom du havner på faddergruppe med noen du ikke kommer så godt overens med, så må du ikke gjøre det an å spørre fadderen din eller faddersjefen om du kan bytte gruppe. Uansett burde du ikke droppe fadderperioden, for det er en fin mulighet til å bli kjent med folk, byen og linjeforeningen. Bare ha litt is, eller Smirnoff Ice, i magen; du må møte et stort nok utvalg med folk før du kan velge din indre sirkel.



● Som helt fersk student kan en ny studiehelg oppleves overveldende. Da kan det være lurt å bruke litt tid på å sette opp et system for å holde oversikt over daglige og ukentlige gjøremål. Et tips kan være å begynne å se på eksamsensett tidlig i semesteret når pensumet gjennomgås i forelesning. Slik kan man få oversikt over hva som er viktig for å forhåpentligvis kunne få en god karakter til slutt.

● I slutten av andre klasse står man plutselig foran noe som for mange er et vanskelig valg: man må velge studieretning. Dette kan virke som en stor forpliktelse for mange, men sannheten er at det ikke er så farlig hvilken linje du velger, alle ender opp med å kunne jobbe med det samme uansett.

● Kokking er ingen skam hvis øvingene ikke er relevante for eksamen eller læringsutbyttet i faget i det hele tatt. Du kan da bruke den ekstra tiden på selvrealisering, koke flere øvinger eller faktisk lære deg pensum skikkelig.



Glasloken

Dyrkes fortsatt

NTNU vokser enda mer

Tekst: Sand Hanemagn

TRONDHEIM – Etter sammenslåing med diverse høyskoler i 2016, er NTNU nok en gang på utkikk etter nye erobringer. Universitetsstyret har derfor, i imperialismens navn, valgt å annexere to nye utdanningsinstitusjoner. Fra og med 2021 kommer Charlottenlund videregående skole og barnehagen på Berg til å være en del av NTNU, med navnene NTNU Charlottenlund og NTNU Berg. På spørsmål om dette svekker NTNUs prestisje og integritet, svarer rektor Banne Org: «Prestisje og integritet mista vi i 1996, så det er åpenbart ikke et problem. Så lenge vi blir større, er det null stress om kvaliteten går ned.»

Abakus får en «ny» komité

Tekst: C.M. Magnus R. Rand

GLØSHAUGEN – Komiteen PR har lenge vært tema for en opphetet diskusjon. Debatten dreier seg om at PR i dag jobber mer med plakater enn såkalt «Public Relations». I lys av dette har nye HS bestemt at komiteen skal bytte navn til «Plakatkomiteen». Nye HS var dog ikke klar over en gammel statutt fra 1986, som kort fortalt sier at «ingen komité kan under noen omstendighet endre navn.» Løsningen ble derfor å legge ned PR med umiddelbar virkning, for å deretter opprette en ny komité med navn Plakatkomiteen. Da Abakus' verdier blant annet er «åpen», vil den nye komiteen så klart følge vanlig opptaksprosedyre. Ingen tidligere PR-medlemmer vil få noen fordel i opptaket. Undertegnede ønsker de gamle PR-medlemmene lykke til og den nye Plakatkomiteen alt vel!»

Nytt fag fra IDI

Tekst: Vegred Erstone

GLØSHAUGEN – På grunn av manglende forståelse blant studentene i digitalteknikk-delen av TFE4101 Krets- og digitalteknikk har ledelsen i IDI bestemt seg for å ta grep. «Vi må nå ut til ungdommen på et språk de forstå», sier instituttleder Johnas Krogvei. «Vi har derfor valgt å innføre emnet TDT1337 Store redstone-strukturer». Studentene vil selvfølgelig ikke bruke Minecraft i dette faget, men en plugin professor Helvard Tøtterfjell har laget til Eclipse.



Utgavens master

Retrieval of Sheep Using Unmanned Aerial Vehicles



Tekst: Marit Gjøstøl Ytterland (M.Sc. 2019), IT-Trainee, Skatteetaten og Tone Kathrine Evrik Winsnes (M.Sc. 2019), Konsulent, ITverket AS

Har du noen gang tenkt på hvor vanskelig det er for bønder å finne igjen alle sauene sine på fjellet om høsten? Kanskje ikke, men det er faktisk mer enn fem prosent av norske sauar som aldri blir funnet igjen etter å ha gått fritt på beite om sommeren. Letingen er tidskrevende og tapene er et økonomisk problem for bøndene, i tillegg til en etisk utfordring. Bøndene har derfor uttrykt et behov for en mer effektiv måte å finne igjen sauene på ved hjelp av moderne teknologi.

Vi begynte på denne oppgaven med den hensikt å bruke enkle datasynmetoder for å analysere dronebilder, og dermed finne den geografiske posisjonen til sauene slik at bøndene enklere kunne finne dem igjen. Tidligere forprosjekter hadde vist at enkle metoder kunne gi gode resultater, men det var viktig å ha et godt datasett.

Dermed dro vi til en gård i Oppdal, lekte oss litt

med en drone, og dro hjem igjen med over 800 bilder. Disse måtte selvagt analyseres manuelt for å kunne måle suksessraten – sauene måtte kategoriseres og telles. Deretter begynte vi å teste ulike metoder på datasettet for å finne sauene – alt fra å lete etter hvite og svarte piksler, til å sammenligne bredde og lengde for en gjennomsnittlig sau og lete etter sauelignende objekter.

Vi bestemte oss for å først fokusere på å finne de hvite sauene, deretter de svarte, og eventuelt de brune dersom noen av metodene viste potensial. Det viste seg at 80 prosent av sauene i datasettet vårt var hvite, og når vi i tillegg visste at sauar elsker å vandre rundt i flokk, var det et fint sted å starte.

Fant vi sauene?

Etter å ha testet utallige metoder på datasettet fikk vi til slutt gode resultater. Ved å kombinere et

bilateral filter med en preprosesseringsmetode kalt dilation, fant vi 97,8 prosent av alle sauene. Dette forutsetter at man regner med å finne hele flokken dersom man finner én av sauene i den. Til tross for dette gode resultatet ble bare 13,5 prosent av de svarte og brune funnet. Grunnen til det er at svarte, og spesielt brune, objekter er vanskelig å oppdage ute i naturen, da de har veldig lik farge som omgivelsene.

Selv om resultatene var ganske gode, vil det være ønskelig å finne absolutt alle sauene, og ikke bare de hvite. Vi hadde også et problem med at metoden vår ikke kunne skille mellom sauar og andre sauformede objekter. I løpet av den våren vi skrev masteroppgaven vår, kom det rimelige droner med infrarødt kamera på markedet. Vi ser derfor for oss at om man hadde kombinert våre metoder med et infrarødt kamera, kunne man fått enda bedre resultater.

readme presenterer:

Hvorfor du skal følge med i DISKMAT og ALGDAT

Forord: Hei alle nye på datatekologi og kommunikasjonsteknologi!

I denne artikkelen er det hyppig bruk av ordet «koke», som i studentsammenheng betyr å bruke en gammel øving for å skrive egen øving.

Velkommen alle førsteklassinger, andreklassinger og eldre som må ta fag om igjen. Dette semesteret kommer dere til å ha noen beryktede fag som dere blir oppfordret til å koke i: Diskret matematikk eller Algoritmer og datastrukturer. For mange kan fagene virke spesielle, overkompliserte og rett og slett unødvendige. Men vi skriver denne artikkelen til deg, for å fortelle deg at du absolutt ikke burde koke deg gjennom disse fagene, men heller følge med og gjøre en god innsats.

Merk: Dette er en seriøs artikkel, selv om den kan virke litt sarkastisk!

Diskret matematikk

Diskret matematikk, populært kalt *diskmat*, er et ganske spesielt fag, i og med at det inneholder mye som er på grensa til å ikke kunne bli kalt matematikk. Det kan føles ut som om det er mange grunner til å ikke følge med: Mange av forelesningene er så som så, øvingsopplegget ligger ute på YouKok, og mange av oppgavene i øvingsopplegget er så rare og vanskelige at man enten ikke har peiling på hva det spørres om, eller at man må bruke et helt semester på å bevise at det er $a_{n-1} + a_{n-2}$ måter å gå opp en trapp på. I det hele er det et ganske *kokbart* fag.

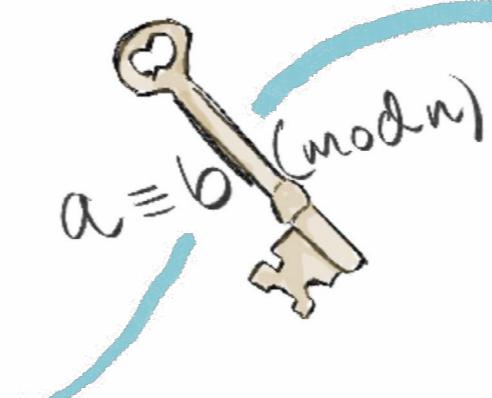
Allikevel forteller jeg deg nå at du ikke bør koke deg igjennom diskmat. Hvorfor det? Hva kan man oppnå med å faktisk gjøre øvingsopplegget? Kan man ikke bare øve før eksamen? Det som er tingen med diskmat, og som ofte er greia med flere fag, er at kunnskapen må *modnes*. Mange konsepter og oppgaver kan virke ulogiske når du først hører om dem, men dersom du gjør oppgaver du ikke skjønner og venter en stund, kan det ofte være at du skjønner konseptene når du kommer tilbake til samme oppgave. Det er nesten magisk.

Diskmat kan også sies å ha et eget språk. Måten oppgaver formuleres på, og hvordan setninger er bygd opp i diskmatboka og eksamsoppgavene er mildt sagt spesielle. Første gang du ser oppgavene vil du ikke ha peiling på hva det faktisk spørres om. Men etter hvert som du gjør flere og flere oppgaver, vil du forstå hva som menes i de overkompliserte oppgavene.

Et av kapitlene som er ekstra viktig å følge med på er kapittelet om modulo. Modulo er et ekstremt viktig konsept i programmering, spesielt sikkerhet. Dersom du setter deg inn i hva modulo handler om, og hvorfor og hvordan det brukes, vil du ha en god fordel i resten av studiet.

Et eksempel på dette er når dere skal lære om RSA. RSA går igjennom diskmat, men selve grunnlaget rundt hvordan RSA fungerer kan du lære hvis du kan modulo.

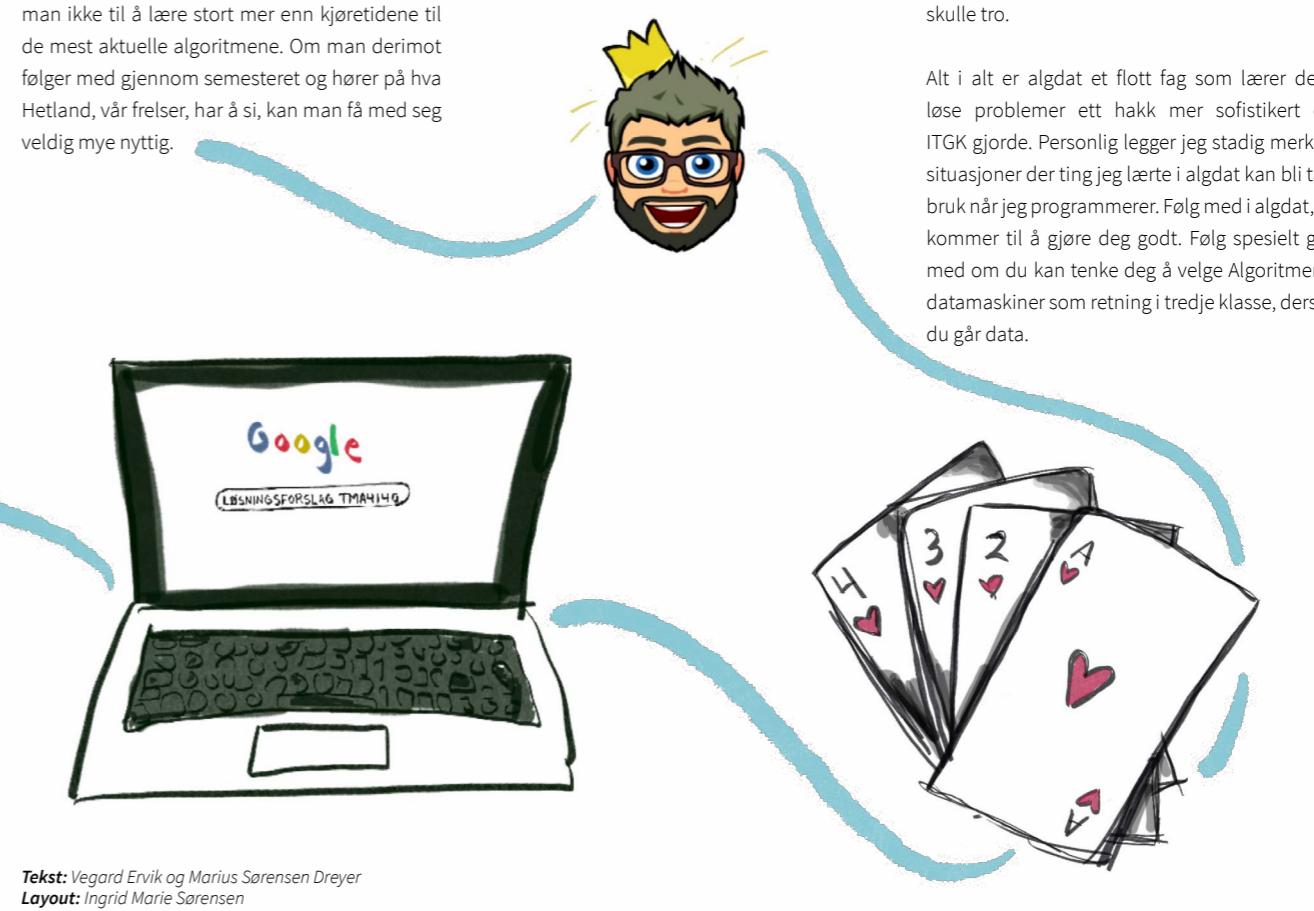
Til slutt vil jeg bare si: omfavn diskmat. Går du inn for å like faget, vil du kose deg med å øve til eksamen. I tillegg er det et fag som mye programmeringsteori bygger på. Om du forstår dette faget godt, har du en stor fordel videre i studiet!



Algoritmer og datastrukturer

En løk har mange lag. Det sa Shrek. Noe som også har mange lag er emnet *algdat*. Hver gang man tror man har lært noe, kan man skrelle av et nytt lag og lære noe mer. Om den sammenligningen gir noe mening, er opp til den enkelte. Uansett er algdat ansett som et veldig godt fag, og her kommer noen gode grunner til at du skal følge med i forelesningene det kommende semesteret.

Algdat er veldig nyttig. Man lærer veldig mye om forskjellige algoritmer og hvordan de kan brukes, hvordan man kan strukturere data effektivt og om hvordan kompleksitet vokser med størrelsen på *input*. «Men hvorfor må jeg kunne implementere og huske kjøretider til algoritmer jeg lett kan *google* eller installere med *pip install algorithms*? Nei, nå skal du høre. Noe av det viktigste å forstå med algdat er at det lærer deg *problemløsning*, ikke kun hvordan hver enkelt algoritme fungerer. Selvfølgelig, om man tar algdat på én uke rett før eksamen kommer man ikke til å lære stort mer enn kjøretidene til de mest aktuelle algoritmene. Om man derimot følger med gjennom semesteret og hører på hva Hetland, vår frelses, har å si, kan man få med seg veldig mye nyttig.



Tekst: Vegard Ervik og Marius Sørensen Dreyer
Layout: Ingrid Marie Sørensen

Å ha forståelse for hvordan algoritmene fungerer individuelt legger grunnmuren for å skjønne hvordan de kan fungere sammen og i nye problemer man ikke har sett før. Eksamens i algdat inneholder alltid noen større forståelsesoppgaver. Disse kommer til å teste hvor god man er til å analysere et nytt problem og lage en algoritme som løser problemet på en korrekt måte. Man får mye igjen for å gå i forelesning i algdat, ettersom man får de viktigste aspektene ved en algoritme forklart rolig og oversiktlig. Hetland er vanvittig flink til å lage oversiktlige presentasjoner.

Forelesningene fokuserer mye på algoritmene, men øvingene er mer praktisk rettet og får deg til å se disse algoritmene i et nytt lys. Prima trening om man vil skjønne hvordan forskjellige algoritmer henger sammen, og hvilke problemer de løser. Rett som det er må man kombinere to eller tre algoritmer for å finne korrekt løsning på et problem, og det er ikke alltid så lett som man skulle tro.

Alt i alt er algdat et flott fag som lærer deg å løse problemer ett hakk mer sofistikert enn ITGK gjorde. Personlig legger jeg stadig merke til situasjoner der ting jeg lærte i algdat kan bli tatt i bruk når jeg programmerer. Følg med i algdat, det kommer til å gjøre deg godt. Følg spesielt godt med om du kan tenke deg å velge Algoritmer og datamaskiner som retning i tredje klasse, dersom du går data.



STEAMY SPILL

DR PINKCAKE PRESENTS

BEING A DIK

Om du gamer på PC, er du sannsynligvis kjent med den digitale spill- og distribusjonsplattformen Steam. Steam tilbyr titusener av spill fra alle mulige sjangre, også spill med voksent innhold. Ved første øyekast kan det virke som om spillene merket med «Sexual Content» ikke er mer enn middelmådig hentai innpakket i dårlige 2D-spill. Finnes det egentlig gode spill i jungelen av adult-juggef?

Tittel: Being A DIK

Redaksjonens vurdering: **Blandet**

Anmelders vurdering: **Overraskende positiv**

Utvikler: En ganske sjuk fyr

[Er dette spillet noe for deg? Les videre ➔](#)

A Study in Pink

Bare det å finne noe som ser *lovende* ut er en oppgave i seg selv – i skrivende stund er det 2245 spill å bla gjennom. Blant disse finner man titler som «OshiRabu: Waifus Over Husbandos», «Hentai Nazi HITLER is Back» og noe tvilsomme «Sisterly Lust». Sistnevnte er kanskje best å la ligge.

Visuell roman

Det finnes likevel noen lyspunkter. «Max Gentlemen Sexy Business» virker som om det har litt produksjonskvalitet. Det samme gjelder «Acting Lessons» og «Being A DIK» – begge fra samme utvikler, DrPinkCake. Kan dette være vårmann? Anmeldelsene til begge spillene hevder at historiene er engasjerende og velskrevne, og at valgene man tar er meningsfylte. En «Acting



Lessons»-spiller hevder at han «came for a fap – left with heavy emotional scarring and complete sense of insignificance». Dette kan være verdt å sjekke ut. I «Being A DIK» tar man visstnok rollen som en «freshman» ved et amerikansk College – en setting som vel passer perfekt for den gjengse abakule. La oss gi det et forsøk.



ligger mellom ytterpunktene «Massive CHICK» og «Massive DIK», og valgene man tar drar hovedpersonen i en av retningene. Underveis i historien dukker det også opp såkalte «major choices». Disse er mer definerende for hovedpersonen i tillegg til at de gjerne har større innvirkning på selve historien. Hvor man ligger på DIK-skalaen kan også begrense eller åpne opp for valgmuligheter for spilleren. En gang var for eksempel ikke karakteren min «chick» nok til å gi en klem til en jente.

Handlingen

Selve historien kan i grove trekk minne om *American Pie* med humor, sex-fokus, og typisk college/high school-drama, men det har også en rekke seriøse undertoner som man kanskje ikke forventer å finne i et spill som dette.

Spillet følger hovedpersonen gjennom de første ukene – fadderperioden om du vil – på college. På grunn av uforutsette hendelser blir han stående uten sted å bo, og ser seg nødt til å *pledge* hos et av broderskapene på colleget: Delta Iota Kappa – DIK. Det er imidlertid ikke bare bare å få innpass i et broderskap, og etter kort tid er hovedpersonen og hans nye makker Derek midt i en opptaksprosess som får Abakus' dresskledde sakseklippere til å se ut som Moder Teresa.

Som DIK-pledge blir man raskt introdusert for de andre broterskapene, som tikker alle boksene et stereotypisk college må ha. Man har «the Nerds», glosingenene; «the Preps», pretensiøse handels-folk; «the HOTs», partyjentene; og «the Jocks» de vektløftende testo-bombene som DIK selvfolgelig har *beef* med fordi noen *hooka* med dama til noen – *classic*.

Man møter et flust av karakterer som stort sett er velskrevne og troværdige. Til tross for at mange av dem har en stereotyp-rolle å fylle, får man inntrykket av at de faktisk er flerdimensjonerte mennesker – særlig ultra-jocken Chad, som ved første øyekast synes å være nettopp bare en ultra-jock, viser seg å være mer enn som så.

Dialogen – som det meste av handlingen er bygget opp av – er både underholdende og har en naturlig flyt; replikkene føles ikke påtvungne og man får aldri inntrykket av at historien dras ut – til tross for at spillet faktisk tar 10-12 timer å komme gjennom. DIK-makkeren Derek har hovedrollen i flere komiske scener, og ble i løpet av de 10 timene en karakter jeg brydde meg mer om enn de fleste i siste sesong av *Game of Thrones*.



«Handlingen»

Det er umulig å unngå seksuelt innhold når man spiller spill merket med «sexual content», men jeg skulle nesten ønske man kunne det – i alle fall til en viss grad. Pupper og sex leder an i promoteringen på spillets Steam-side; selv om det ikke er direkte misvisende, viser det bare en brøkdel av hva spillet har å tilby, og er samtidig nok til å få de aller fleste til å avskrive spillet fullstendig.



Sex i spill er i og for seg ikke noe problem: Bøker, filmer, TV-serier og spill har alle utallige eksempler på sex-scener med varierende kritikker. Felles for dem alle er dog at de gjerne benytter seg av teknikken «Fade to Black» på strategiske tidspunkter for å unngå å vise absolutt alt. Det gjør ikke «Being A DIK». Enten du vil det eller ei, presenteres du flere scener som ikke kan beskrives som annet enn pornografi. Disse dukker ikke bare opp naturlig som følge av hovedpersonens handlinger – de som ikke er det kan finne sted en helt annen plass eller være en av hovedpersonens flere dagdrømmer, og virker derfor ganske påtvungne. De øvrige scenene passer inn i den grad de er en naturlig prosesjon av historien (selv om det kan virke i overkant lett å få seg noe i dette universet), og påvirker slikt sett ikke narrativet negativt – man risikerer likevel å trekkes ut av selve spillopplevelsen for å klikke seg gjennom bilder og animasjoner i et lite minutt.

Konklusjon

Nøyaktig hva jeg forventet da jeg startet «Being A DIK» vet jeg ikke, men det var i hvert fall ikke en god historie og et karaktergalleri som jeg skulle bli investert i. Spillet står stødig på egne ben selv uten sex-scenene, og hadde det blitt sensurert ned til et fjernsynsvennlig nivå, ville jeg ikke nølt med å anbefale det. Tolk det som du vil, men om du er nysgjerrig på en spillopplevelse litt utenom det vanlige – og ikke har noe imot å klikke deg gjennom litt porno i ny og ne – kan det være verdt å gi det et forsøk.

Foto og layout: Magnus Hanesand, Marius
Sørensen Dreyer og Henrik Fauskanger



STRATEGEN™



Ting du bør vite som siving

WSL

Tekst: Andreas Hammer Håversen

Det er ikke til å legge skjul på: Linux er det beste operativsystemet som finnes for utvikling, og har vært det lenge. De av oss som sverger til Windows har et forklaringsproblem. Terminalen vår suger, vi har ingen innebygd pakkebehandler, og «/»-ene våre går feil vei. Nei, det er ikke lett å være det sorte fåret i utviklerfamilien. Heldigvis kan ikke Linux-brukerne le like høyt lenger. Nå kan du nemlig kjøre Linux i Windows, helt uten virtuelle maskiner eller annet rot. Det er ren glede.

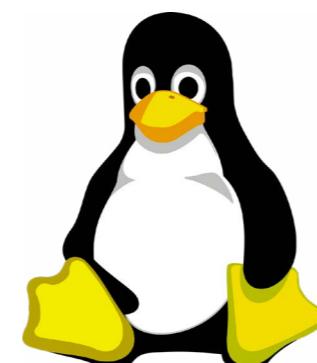
La meg introdusere deg for Windows Subsystem for Linux (WSL), din nye bestevenn. Enkelt forklart er dette et system som lar deg kjøre Linux-programmer i en *bash*-terminal som om du var på en Linux-maskin, fra en Windows-terminal. Rent teknisk innebærer dette at Windows pakker Linux-programmene dine inn i et kompatibilitets-lag som oversetter programinstruksjonene til noe som kan kjøres av Windows. Dette gjør at man kan nyte full ytelse i Linux-miljøet, til tross for at alt kjører i Windows. Sammenlignet med det å kjøre Linux i en virtuell maskin er dette ganske revolusjonerende.

Keiserpenguinens kongelige terminal

Det tekniske til side, hvilke fordeler gir det egentlig å bruke WSL? Den mest umiddelbare forbedringen

opplever man i terminalen. Linux har jevnt over mye bedre støtte for bruk av kommandolinjen. Den største åpenbaringen undertegnede fikk, var oppdagelsen av *alias*. Et alias er en kortform av en kommando som man kan lage og bruke i terminalen. Det gjør at man for eksempel kan forkorte **npm install** og **npm run serve** til **ni** og **ns**. Om du går for den førstnevnte blir du medlem av den meget eksklusive klubben «The developers who say *ni!*». Dette kan også utvides til å kjøre egenproduserte bash-skripter for utrolig mange forskjellige oppgaver. Tilpasningsmulighetene er kort sagt uendelige.

Oppsummert gjør WSL det mye enklere å være utvikler på Windows. Det er lett å installere, og takket være en tett integrasjon mellom WSL, Visual Studio Code og nye Windows Terminal får man i sum en svært god utvikleropplevelse. *Windows is back, baby.*



Pingvinens bakside

Dessverre er det ikke alt som fungerer helt som det ville gjort i ekte Linux. En av utfordringene er at man ikke kan bruke grafiske Linux-applikasjoner i WSL

Ting du ikke trenger å vite som siving

Vørterøl

17



Tekst: Vegard Ervik

Fremtiden til vørterøl

Det er ingen tvil om at vørterøl ikke er så stort som det en gang var. Rundt 1950 sto vørterøl for 13 prosent av ølkonsument i Norge, mens i dag står det for mindre enn 1 prosent. Allikevel mener jeg at vørterøl har mye potensial og kan komme tilbake i fremtiden. Ifølge Ringnes brukes i dag vørterøl på intensivavdelinger og fødestuer. Det selges mye til treningsenter og aldershjem. I tillegg stimulerer det melkeproduksjonen hos ammende. Siden dette kommer direkte fra Ringnes, bør det taes med en klype salt. Men både malt og humle har påvist gode helseeffekter, som at det hjelper mot sovnloshet, depresjon og hjelper med fordøyelsen. Nå som vi har sett at vørterøl er godt for kroppen, er det viktig at det må være godt for sjela. Så for å nyte vørterøl best mulig bør du helle det i et glass, kaldt fra kjøleskapet. *Bon appétit!*



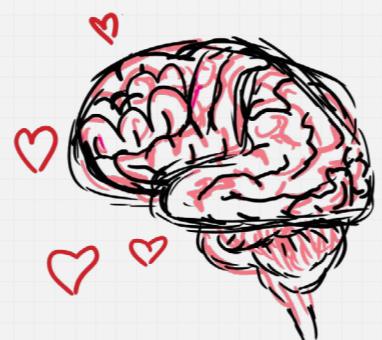
Mastergrad på autopilot -EN GUIDE

Tekst: Magnus Hanesand, Magnus Schjølberg og Henrik Fauskanger
Layout: Karoline Sæbø

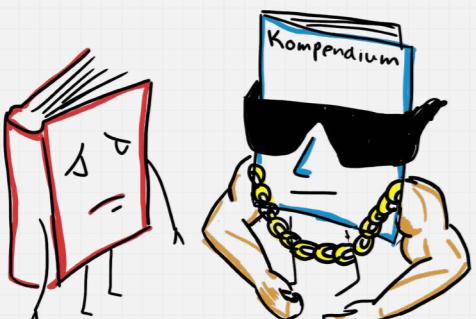
Du har bevist din enorme intellektuelle kapasitet ved å komme inn på et studie med skyhøyt snitt. Det er enormt attraktivt og kan beskrives som en rød løper til en komfortabel og godt betalt jobb. Så nå følger det eneste naturlige – å komme seg gjennom med minst mulig innsats.

Faddergruppa er til for å utnyttes

Du kjenner typen. Rett fra videregående, oppmeldt i syv fag, har progg siden før han kunne spise fast føde. Denne duden er på faddergruppa di, og du trenger ham i arsenalet ditt. Når prosjektfagene dukker opp, må du ha noen på gruppa som kan dra lasset. I disse fagene er det for øvrig en *fordel* å ikke kunne en dritt. Da unngår du å få arbeidsoppgaver helt fra starten av. Din arbeidsoppgave blir da naturligvis innleveringsansvarlig: Du «leser over» når oppgaven er ferdig, og leverer den på Blackboard. Et godt stykke arbeid, kaller vi det.



Bøker er bare kule når de heter kompendium
Boka er dyr. Det er noen hundrelapper du heller kunne brukt på pils et kvarter før Samf stenger. I tillegg tar den både tid og krefter å lese, og er det én ting studenter i 2020 ikke har, så er det tid og krefter. Invester heller i et kompendium. Kompendier er noe vanskeligstilte linjeforeninger selger til trengende abakuler. Sånn sett er dette ditt veldedige bidrag til verden, så kan du med god samvittighet ignorere stakkarene som står på stand for Leger Uten Grenser. Uansett, les kompendiene når det blir undervisningsslutt og du ikke lenger må bruke tiden på å koke øvinger. Hvis du vil ta det ett hakk lengre, kan du attpåtil droppe å kjøpe kompendier og heller bruke Wikipendium, som er skrevet av andre grådige jævler som deg selv. Da lærer du deg akkurat det du trenger for å stå, men ikke noe mer enn det. Det er det vi kaller effektivt.



Kok alt, alltid

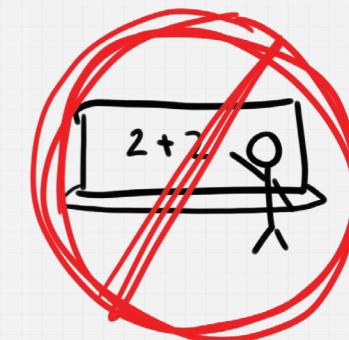
Øvinger er ikke relevante for eksamen. Dette er helt universelt, og gjelder også de fagene der øvingene er relevante for eksamen. For å koke én øving i *matte 1* trenger du 1 liter vann, 10 gram salt og 3 øvinger fra fadderne dine som du kan mikse og matche. Har du dårlig med tid, kan du vurdere å kun bruke én øving – det er ingen studasser som bryr seg uansett. Hvor finner man kok, spør du? I gamle dager brukte vi YouKok, men nå til dags finner du det enklest ved å google. Ofte ligger koken over selve emnesiden i søkeresultatene. Pass bare på å unngå akkurat første søkeresultat, da har du allerede lagt inn mer innsats enn fagstabben legger inn på plagiatsjekk. Har du skikkelige baller av stål, så henter du kok fra GitHub-en til egen studass.

Men vær varsom! Hvis du tenker for mye når du koker, risikerer du å forvirre deg selv, eller i verste fall faktisk lære noe! Grøss.

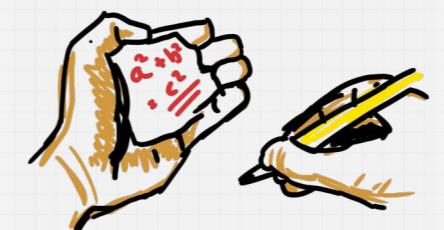


Forelesningene er bare kok de også

Forelesers faglige bakgrunn er ikke eksamsrelevant. Ei heller forelesers hobbyer, familieliv eller mikrofontrøbbel. Gjesteforeleserens spennende historie om hvordan han bruker vakt relaterte teknikker i industrien og med det bedriver *enorm verdiskaping* er – selv om det er *veldig spennende* – heller ikke eksamsrelevant. Eksamensforelesning er kanskje eksamsrelevant. Men bare kanskje.



Shh...



Eksamen kan også kokes

«Koke eksamen? Det er vel ikke greit?» tenker du nå. Og du har helt rett, det er faktisk juks. Men å koke øving er også juks, så den salaten har du på en måte tråkket i allerede. Kokking er det som på fransk kalles en «gateway drug», så veien til eksamensjuks og intravenøs heroinmisbruk er ikke så lang. Alle triksene du husker fra videregående funker fortsatt, bare prøv å være litt mer diskré enn kidsa på VGS som juksa for å sikre seg 3-ern i tysk.

Obs! **readme** er ikke ansvarlig for utestengelse, skade, moralisk forfall eller død som følge av juks på eksamen. Hvis alle forslagene over skulle feile, så er det bare å spise litt flaggermus og forårsake en internasjonal pandemi, så blir alle skriftlige eksamener hjemmeeksamener.

En **readme** til bedpres!

Vil du lære mer om jobbmulighetene dine etter studiet, knytte tettere bånd med arbeidslivet, eller har du rett og slett bare lite igjen på middagsbudsjettet denne måneden? Da bør du ta med deg noen medstudenter og dra på bedriftspresentasjon!

Hva er en bedpres?

En bedriftspresentasjon, ofte kalt *bedpres*, er et arrangement der bedrifter samler studenter for å presentere seg selv og hva de driver med. Dette etterfølges som regel av mingling med mat og drikke sammen med bedriftsrepresentantene (kalt *bedrepper*). Hvis du har ubesvarte spørsmål om bedriften etter presentasjonen, er minglingen etterpå den perfekte muligheten til å finne svar. Eventuelt kan du heller bare drikke deg snydens.

Hvordan finne bedpresser?

Første stopp for å fylle kalenderen med bedpresser er naturligvis *abakus.no*, men det arrangeres også en rekke bedpresser uavhengig av linjeforeningene. For eksempel arrangeres det flere forskjellige næringslivsdager, som itDAGENE, Nettverksdagene og Tech Talks med spennende bedpresser på kveldstid. Det lønner seg også å følge med på oppslagstavler, Facebook-arrangementer og nettsidene til blant annet Teknologiporten og Start NTNU for å få med seg bedpresser med linjeavhengig påmelding. Ofte er det trangt om plassene på bedpressene, spesielt på *abakus.no*, så her gjelder det å sitte klar i det sekundet påmeldingen åpner.

Gira på jobb?

Do: Sosialiser deg, vis interesse, og snakk om egne prosjekter som viser engasjement
Don't: Skift tema bort fra bedriften og hvor kult det er å jobbe der



Gira på fylla?

Do: Få en god tone med bedreppene tidlig på kvelden for ekstra bonger
Don't: Sett deg med bedreppen som ser ut som de heller ville vært hjemme og som drar tidlig



Gira på en kveld med venner?

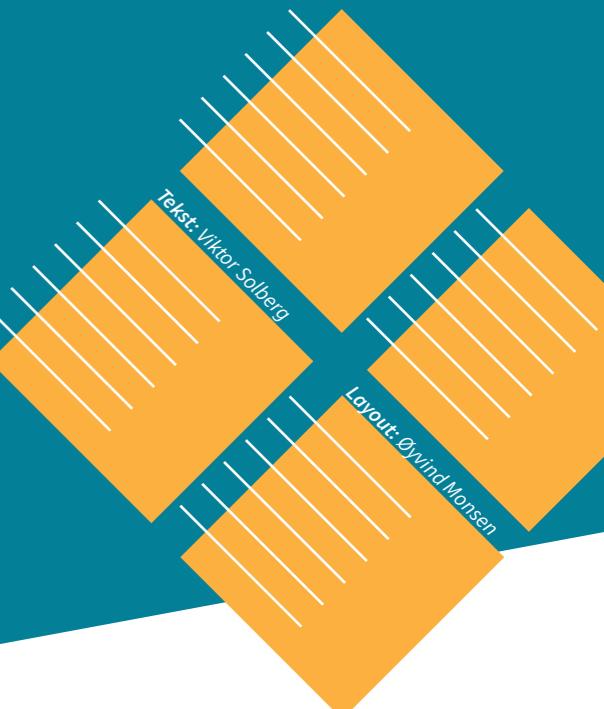
Do: Vær tidlig inne på bespisningsstedet og finn et godt bord med vennene dine
Don't: Utelat bedreppen fra samtalen



Når man først har satt seg, finner man fort ut at man blir sittende ved det samme bordet hele kvelden. Hvis du går i første eller andre klasse, så kommer du nok også til å merke at du vil bli totalt ignorert etter at bedreppen har «tatt runden» og spurte hvilket trinn alle rundt bordet går. Den uetiske *lifehacken* her er derfor å ikke sette seg med de femteklassingene du egentlig aldri har sett før, da bedreppen kommer til å bruke all tiden sin på å rekruttere disse. Sett deg heller med kun folk du kjenner, eller i alle fall går på samme trinn med. Da har ikke bedreppen noe annet valg enn å sosialisere med dere, og da slipper dere å sitte der tørste og bongløse.

LIVET ETTER KORONA

Mars i år viste seg å være en merkverdig måned. Endelig fikk Erna lov til å gjøre det hun liker best, nemlig å utøve makt, ved å stenge ned hele Norge. Plutselig var det ikke lenger greit å dra på hytta, og utepils i parken ble ulovlig på ordentlig. Mange av oss hadde dermed ikke annet valg enn å venne oss til et liv innendørs i isolasjon. Dette høres egentlig ikke så ille ut, spør du meg, men det er pussig nok mange som ser frem til en mer normal hverdag igjen. **readme** har derfor gløttet inn i krystallkula for deg. Her kommer noen spådommer for hvordan verden vil utvikle seg etter koronakrisen:



Vi må begynne å bruke bukser igjen



Null fleip! Dette skjer som en konsekvens av at vi ikke lenger kun vil se hverandre gjennom en PC-skjerm. Når både Zoom og Discord opphører som våre naturlige møteplasser, vil vi nok en gang måtte møte hverandre ansikt til ansikt – helst i full påkledning. Det finnes også andre interessante konsekvenser som kan være verdig å merke seg – spesielt for den jevne abakule. Den viktigste konsekvensen å tenke over er kanske at det ikke lenger vil være like akseptabelt å ta seg en pils eller fire uten fysisk selskap.

Helsevesenet bukker under



Denne spådommen virker nok paradoksal for de fleste. Hvorfor i alle dager skulle helsevesenet gå dukken etter koronakrisen? Vel, det som nå har skjedd er at alle koronatiltakene har medført en mengde stillesitting man aldri tidligere har vært vitne til. Stillesittingen vil igjen føre til en bølge av livsstilssykdommer som kommer til å skylle inn over Norge, og til slutt ta knekken på hele det norske helsevesenet. Kanskje tiden endelig er moden for å sanke inn et par kilometre på Strava?

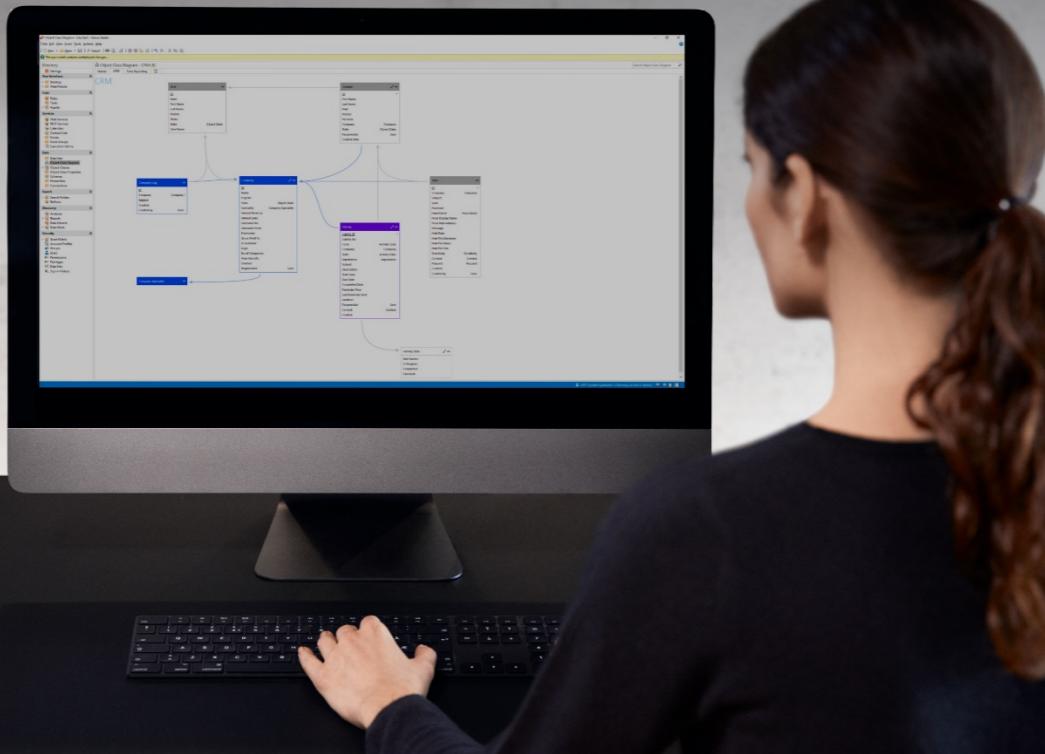
Overbefolking på A-blokka

Er du av typen som synes det er trangt om plassene på A-blokka den dag i dag? Da vil du grøsse av tanken på plassmangelen som våre etterkommere vil måtte oppleve – om sånn omrent 19 år. Dette vil skje på grunn av et velkjent fenomen som kommer til å finne sted etter koronakrisen, *babyboom*.



Hva nå?

Selv om alle nevnte spådommer helt sikkert kommer til å slå til, er det ingen grunn til å se mørkt på livet. Når koronatiltakene oppheves, burde vi alle heller oppmuntre hverandre ved å bidra til en lysere hverdag. Dette kan vi gjøre ved å venne oss til å ikke lenger se rart på folk som opptrer nærmere enn to meter fra hverandre i offentligheten, eller ved å slutte å true hytteglade folk på livet.



Genus er et norsk softwareselskap som leverer en ledende [low-code plattform](#) for utvikling av virksomhetssystemer.

Gjennom visuell modellering lar plattformen deg utvikle avanserte forretningssystemer [uten behov for tradisjonell programmering](#). Dette gir økt utviklerproduktivitet, lavere kostnader og mer fleksible og bærekraftige løsninger.

Genus kommer til Trondheim 27. august

Torsdag [27. august](#) vil Genus avholde bedriftspresentasjon for Abakus linjeforening. Vi kan love spennende presentasjon med god mat og drikke i løpet av kvelden. Dere vil møte hyggelige bedriftsrepresentanter som er interessert i å bli kjent med akkurat deg. Se [abakus.no](#) for påmelding.

Håper vi ser deg der!

Mer info?

[genus.no](#)

Søke?

[recruit.genus.no](#)

Instagram

@genusbiz



Løse komplekse problemer i sommerjobben din neste år?

[capraconsulting.no/karriere/sommerjobb](#)

C
A P R A



Jobbe i en tech startup?

Les mer om summer internship og fast stilling på [appfarm.io/jobs](#)

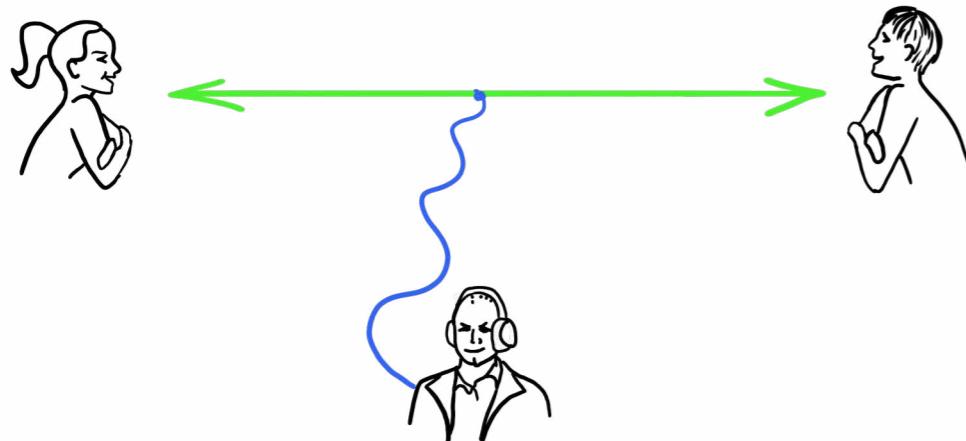


Søknadsfrist 1.oktober

Utgavens Algoritme

Med: Henrik Fauskanger

Diffie-Hellman



Den høyteknologiske verden rundt oss er full av helt utrolig smarte løsninger. Dette gjelder kanskje ekstra mye innenfor kryptografi-feltet. Når vi sender meldinger til hverandre og ikke ønsker at fremmede skal få lese dem, er det vanlig å skjule innholdet i meldingene med kryptering, men hvordan avtaler vi egentlig hvordan meldingen skal krypteres? Det hjelper jo lite å sende krypterte lapper i klasserommet når læreren allerede har hørt oss rope krypteringsnøkkelen. Våre venner Diffie og Hellman har svaret.

Diffie-Hellman Key Exchange (DHE) benytter seg – som mange andre kryptosystemer – av modulær aritmetikk. Teknikken lar to parter regne seg fram til en felles nøkkel, uten at den avtales eller deles eksplisitt over en usikker kanal.

Algoritmen:

1. Jeg bestemmer meg for et primtall p og et tall g som som er *relativt primisk* med $p - 1$. Jeg sender så disse til deg.
2. Du bestemmer deg så for et tall a . Dette tallet forblir i din besittelse, og du bruker det til å regne ut $A = g^a \text{ mod } p$. Du sender så A til meg.
3. Jeg svarer med samme mynt, og finner på et tall b . Jeg sender deg så tallet $B = g^b \text{ mod } p$.
4. Etter å ha mottatt A og B fra den andre, regner vi hver for oss ut $S_1 = B^a \text{ mod } p$ og $S_2 = A^b \text{ mod } p$.
5. Det er her magien kommer inn: Det viser seg at S_1 er det samme tallet som S_2 , og at vi med dette sammen har regnet oss frem til en felles nøkkel, uten at noen ytre part har hatt sjans til å snappe den opp på veien.

Men så hva, RSA?

De som har vært innom KTN underer seg kanskje over hva som er vitsen med dette når man har asymmetrisk kryptering, som for eksempel RSA. Vil ikke dette gjøre den samme nytten? Nja. RSA fungerer slik at den genererer to tall. Én offentlig nøkkel som alle får tilgang til, som kan brukes til å kryptere meldinger som sendes til meg, og én privat nøkkel som jeg og bare jeg bruker til å dekryptere disse meldingene. Vi kan benytte oss av dette på flere måter:

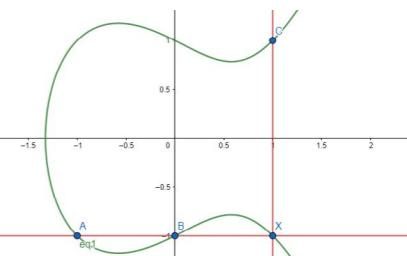
1. Vi kan kryptere hele meldinger med den offentlige nøkkelen vår. Dette krever relativt mye datakraft, og er dermed upraktisk i den virkelige verden.
2. Vi kan kryptere en foreslått nøkkel til en symmetrisk krypteringsalgoritme, som AES, og fortsette kommunikasjonen med denne istedenfor.

Det er her konseptet «forward secrecy» kommer inn: Om en angriper i lang tid har lyttet til nettverkstrafikken min og på en eller annen måte klarer å få grafset til seg min private RSA-nøkkel, vil altså alle disse gamle meldingene også være trivielle å dekryptere. Tenk om noen fikk se alt du gjorde på Facebook da du var tolv år gammel! Skrekks og gru! Om du istedenfor hadde brukt DHE, ville en privat nøkkel aldri kommet på avveie, for den hadde ikke eksistert. Da kunne du vært helt trygg på at de slettede Facebook-postene dine hadde forblitt slettede.

And the curve thiccens

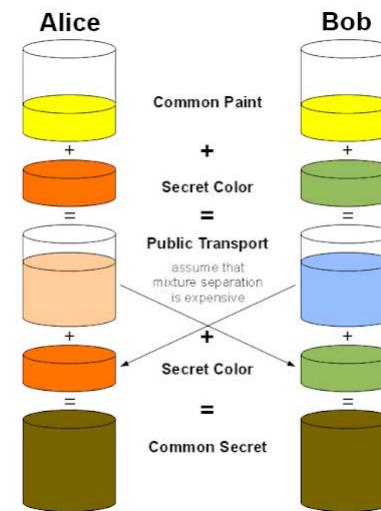
Sikkerheten i DHE baserer seg på at «Integer factorization problem» – altså dekomponering av sammensatte tall til deres primfaktorer – er et vanskelig problem. Den raskeste kjente algoritmen for faktorisering kalles for *General number field sieve* (GNFS), og kjører ikke i polynomisk tid. Kompleksiteten til GNFS er dog subeksponentiell, som gjør den betraktelig raskere enn tilfeldig gjetting.

For å bøte på dette introduserer vi *Elliptic Curve Diffie-Hellman Key Exchange* (ECDHE). I ECDHE bytter vi ut primtallene med punkter på en forhåndsbestemt kurve. Kurven man velger er av det slaget der om man velger to punkter og trekker en linje mellom dem, vil linjen alltid krysse nøyaktig ett punkt til på kurven. For å addere to punkter finner man altså dette tredje punktet, og speiler det så om x-aksen. Ellers fungerer algoritmen omrent likt.



Det å finne ut hvilke to punkter som er ledd i et gitt punkt tilhører «discrete logarithm problem», der den raskeste algoritmen kjører i eksponentiell tid, altså enda treigere enn GNFS. Dette lar oss bruke betydelig mindre nøkler enn i det andre tilfellet, som gjør kjøretiden markant kortere.

Som nevnt innledningsvis er kryptografi-feltet fullt av smarte løsninger, gjerne på problemer du ikke visste at du hadde. Med denne kunnskapen kan du nå sende lapper i klasserommet uten frykt for at læreren leser de klissete kjærlighetsdiktene dine høyt.



Utgavens konkurranse

Sommerjobbende Sivs sløsing

Tekst: Karoline Sæbø

Siv har hatt sommerjobb og liker å skryte over sin nyanskaffede rikdom ved å fortelle hvor mye penger hun har brukt på unødvendige ting den siste uken. Etter å ha mottatt en håndfull klager, innser hun at folk dessverre har begynt å bli lei av denne gjentatte, ensformige skrytingen. For å gjøre det mer interessant bestemmer hun seg derfor for å ikke si beløpet direkte, men heller gi ut hint, slik at den hun snakker med selv kan finne den faktiske summen.

Nå lyder skrytingen som følger:

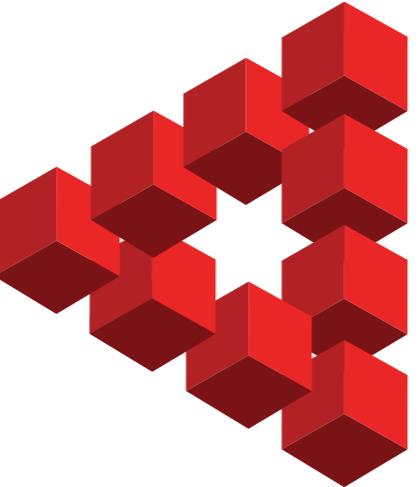
«Når jeg kjeder meg, pleier jeg å summere naturlige tall fra og med én og oppover, slik at differansen mellom etterfølgende tall alltid er én. Hvis fire blir det avsluttende tallet får jeg for eksempel resultatet:

$$1 + 2 + 3 + 4 = 10$$

Og hvis syv blir det avsluttende tallet, får jeg resultatet:

$$1 + 2 + 3 + 4 + 5 + 6 + 7 = 28$$

Hvis du sammenlikner resultatene av slike summer vil du oppdage at 28 er det første resultatet som har mer enn fem divisorer (28 er delelig med 1, 2, 4, 7, 14 og 28). Beløpet jeg sloste bort forrige uke er det første resultatet som har over 97 divisorer.»



Finn ut hvor mye penger som ble kastet ut av vinduet forrige uke, og send inn svaret til konkurranse@abakus.no med emnet «SSS»!

Svarer du riktig er du i tillegg med i den årlige trekningen av en middag for to til en verdi av 2000 kr.

sponset av Genus

Vinnere

1. Andrine Bergan
2. Åsmund Haugse
3. Odd André Owren

Premier

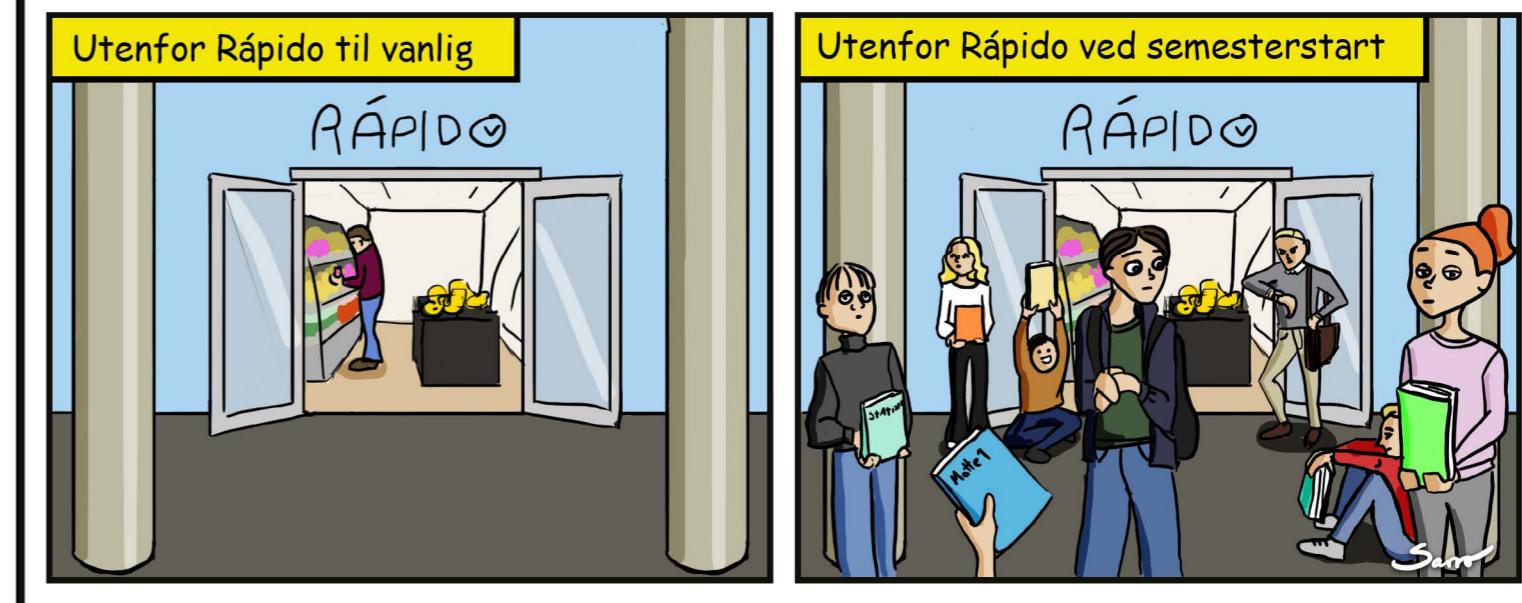
1. premie



2. premie



3. premie



Smått & nett



- det du leser først!

Sykepleierne vender tilbake

readme kunne i fjor rapportere om to abakuler som hadde søkt seg inn på sykepleierstudiet for å kunne delta i Nutrix' fadderperiode. Ryktene skal nå ha det til at de fremtidige sykepleierne ikke hadde fått nok, og har ønsket fjerdeklassingene tilbake med åpne armer. **readme** ønsker wannabe-sykepleierne våre lykke til med å gi førsteklassingene i Nutrix en ordentlig velkomst.

Dobbel nedstenging

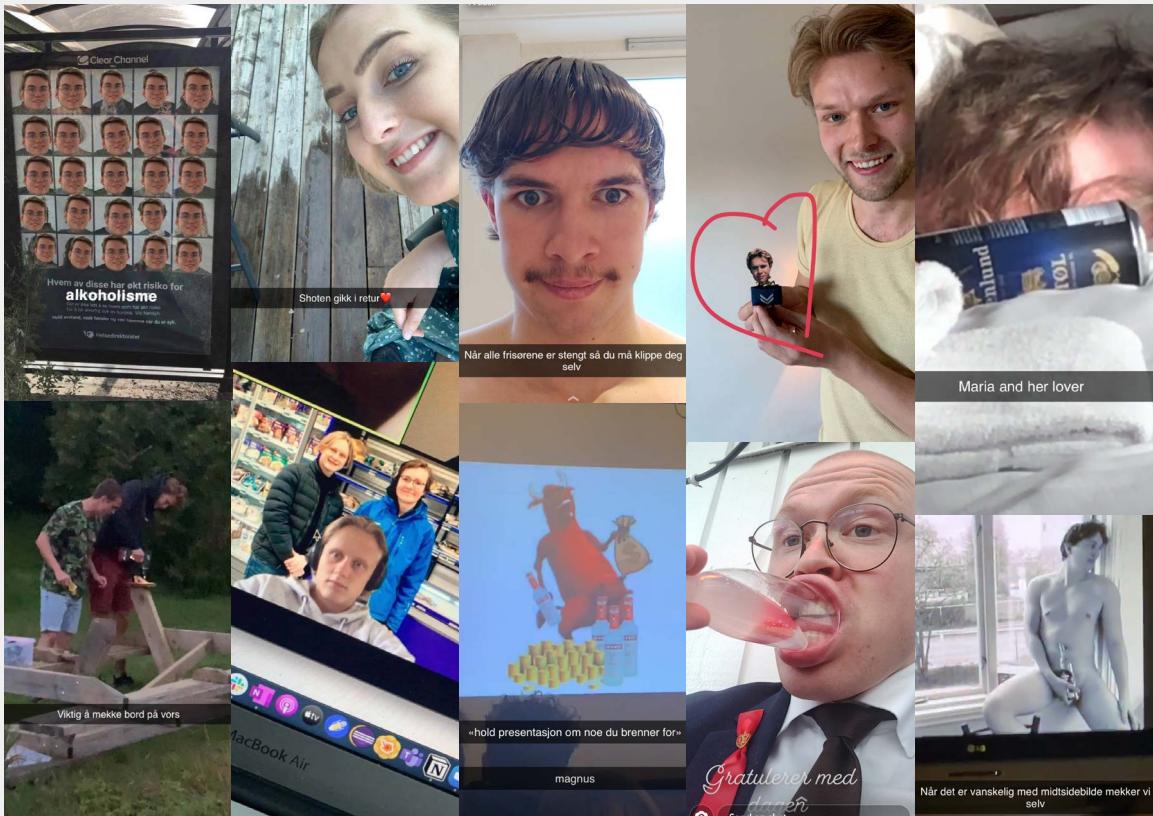
Som om samfunnets nedstengning i mars ikke var stressende nok, fikk Media-gruppen noe ekstra å styre med da Facebook bestemte seg for å stenge ned alt på sine nettsider som hadde med Abakus sin hjemmeside å gjøre. Et av verdens største IT-selskaper hadde altså erklært krig mot linjeforeningen vår og svartelisted alle poster som var lenket til *abakus.no*. Det måtte over to uker med iherdig spamming av kundeservice og kontakt med abakuler i selskapet til før Facebook igjen godtok vår tilstedeværelse.

Koronakos

I begynnelsen av koronatiden skal flere norske medier ha rapportert om uvanlig mye import av dildoer fra utlandet. Redaksjonen kan bare spekulere i opphavet til den markante økningen, men utelukker ikke at kilden finnes internt i Abakus. Hvorvidt det er snakk om single abakuler som savner Bodegaen eller en viss tidligere økonomiansvarlig som sliter uten styrebånd, er derimot ukjent.

Ikke så sosialt distansert

Abakus sin sommerfest bød på mange muligheter for sosialt samvær som ikke var helt i tråd med rådene til FHI. Blant annet skal en andreklassing og en førsteklassing fra data ha hatt det svært koselig på Youngs. Gutten ble observert med en hånd godt plantet under skjørtet til jenta, som svarte med svært positive reaksjoner. Seansen tok først slutt da en annen abakule gikk bort og rådet turtelduene til å fortsette moroa hjemme.



Send tips til
tips@abakus.no

Tidligere utgaver:
readme.abakus.no

Vil du ha snap på baksiden? Send snap til **RYKTE!**

